ice of the Legislative Auditor

State of Montana

Report to the Legislature

November 1994

EDP Audit Report

Information Processing Facility and Central Applications

Each year the Office of the Legislative Auditor audits the state's central computer facility and centralized computer applications. This report is used by financial-compliance and performance auditors and contains our conclusions and/or recommendations for improving general controls over the mainframe computer (Information Processing Facility) and application controls over the following systems:

- State Payroll System
- Statewide Budgeting and Accounting System
- Warrant Writer System

Direct comments/inquiries to:
Office of the Legislative Auditor
Room 135, State Capitol
PO Box 201705
Helena Montana 59620-1705

94DP-33

EDP AUDITS

Electronic Data Processing (EDP) audits conducted by the Office of the Legislative Auditor are designed to assess controls in an EDP environment. EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business and public administration and computer science.

EDP audits are performed as stand-alone audits of EDP controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of four members of the Senate and four members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Greg Jergeson, Chairman	Representative John Cobb, Vice Chairman
Senator Gerry Devlin	Representative Ernest Bergsagel
Senator Eve Franklin	Representative Linda Nelson
Senator Tom Keating	Representative Robert Pavlovich

Office of the Legislative Auditor

EDP Audit

Information Processing Facility and Central Applications

Members of the audit staff involved in this audit were: Bill Kuhl, Rich McRae, Paul O'Loughlin and Patti J. Robertson.

STATE OF MONTANA

Office of the Legislative Auditor

STATE CAPITOL
PO BOX 201705
HELENA, MONTANA 59620-1705
406/444-3122
FAX 406/444-3036

LEGISLATIVE AUDITOR:
SCOTT A. SEACAT

LEGAL COUNSEL:
JOHN W. NORTHEY

DEPUTY LEGISLATIVE AUDITORS:
MARY BRYSON
Operations and EDP Audit
JAMES GILLETT
Financial-Compliance Audit
JIM PELLEGRINI
Performance Audit

November 1994

The Legislative Audit Committee
of the Montana State Legislature:

This is our EDP audit of controls relating to the state's centralized data processing systems operated by the Department of Administration and the State Auditor's Office. We reviewed the Department of Administration's general controls over the Information Processing Facility and application controls over State Payroll and the Statewide Budgeting and Accounting System (SBAS). In addition, we reviewed application controls over the Warrant Writer system, operated by the State Auditor's Office. This report contains recommendations for improving EDP controls related to SBAS, State Payroll, and Warrant Writer systems and the Information Processing Facility. Written responses to our audit recommendations are included in the back of the report.

We thank the Department of Administration and State Auditor's Office for their cooperation and assistance throughout the audit.

Respectfully submitted,

Scott A. Seacat
Legislative Auditor

Table of Contents

Appointed and Administrative Officials

Department of Administration	Lois Menzies, Director
	Connie Griffith, Administrator Accounting and Management Support Division
	Terry Atwood, Chief, Accounting Bureau
	Tony Herbert, Administrator Information Services Division
	Jeff Brandt, Chief Policy, Development, and Customer Relations Bureau
	Paul Rylander, Chief Computing Operations Bureau
	Mark Cress, Administrator Personnel Division
	John McEwen, Chief Classification and Pay Bureau
	Donna F. Warner, Supervisor State Payroll
State Auditor's Office	Mark O'Keefe, State Auditor
	Dave Hunter, Deputy State Auditor
	Thomas L. Crosser, Deputy Fiscal Control and Management Department

Report Summary

Introduction

Our EDP Audit reviewed centralized controls over the state's mainframe computer and the State Payroll, Warrant Writer, and the Statewide Budgeting and Accounting System (SBAS) computer based applications. We performed a general control review of the state's mainframe computer and application reviews of State Payroll and SBAS, each operated by the Department of Administration. We also performed an application review of Warrant Writer which is operated by the State Auditor's Office. A discussion of general and application controls is included on pages 1 and 2. The objectives and scope of the audit are discussed on page 3 of the report.

General Controls

The Department of Administration's Information Services Division (ISD), manages central data processing services for use by state agencies. Central data processing services include: central mainframe computer processing; design, development, and maintenance support of data processing applications; and disaster recovery facilities for critical data processing applications. Processing is performed on an IBM 3090 computer operating 24 hours a day.

We found ISD's general controls provide for controlled application processing on the mainframe computer system. However, we identified physical security and electronic access control issues which could compromise ISD's ability to provide continuous processing services. Summarized below are two examples of how ISD could improve physical security controls over its data processing services. Additional discussion of these and other issues is included in Chapter II of the report.

ISD Should Complete a Disaster Recovery Plan

We determined ISD has not completed a recovery plan or included agency applications in its recovery procedures. Since contracting with Weyerhaeuser Corporation for hotsite recovery, ISD's Computing Operations bureau has placed priority on recovering mainframe hardware, operating system software, and telecommunications. However, these services could not be utilized following a disaster unless state agencies establish hotsite

recovery procedures for their mainframe application programs and data.

We believe ISD should complete its disaster recovery plan by including agency applications and documenting recovery procedures. ISD employees indicated the department has established procedures to complete a recovery plan by June 1995. The director of the Department of Administration, with assistance from the Information Technology Advisory Council, should identify and establish priorities for applications which must be recovered to continue state government operations following a disaster.

Restricted Access to the Information Processing Facility should be Improved

We reviewed ISD's physical security controls which limit access to the computer facility to authorized individuals. We found one of ten employees no longer required access, because the employees' job duties had changed. We also determined individuals, who do not work for ISD, could bypass the computer facility electronic access system by using a grandmaster key at the facility entrance. The department's General Services division issues grandmaster keys to contractors and non-ISD employees for access to several buildings within the capital complex.

EDP guidelines suggest management restrict access to the computer facility to individuals who require access to perform job duties. We believe ISD should establish procedures to remove employee access as soon as no longer required. Following our review, ISD employees noted the division changed the locks to the computer facility to restrict unauthorized access with the grandmaster key.

Application Controls

We performed application reviews of the SBAS, State Payroll, and Warrant Writer. Overall, we concluded the controls over the applications are adequate to ensure data integrity. However, we found areas where SBAS and State Payroll application controls could be improved to ensure continued data security and integrity. Our audit issues are summarized below and discussed in further detail in Chapter II.

The Accounting Bureau should Establish Formal Procedures

During fiscal year 1993-94, the Accounting Bureau periodically released warrants for Department of Commerce and the State Compensation Mutual Insurance Fund when the accounting entity cash balance was negative. Accounting Bureau personnel indicated they released warrants upon verbal agency request contingent upon subsequent cash receipt.

The Accounting Bureau's current procedure may allow inappropriate fiscal activity by state agencies. We believe the Accounting Bureau should document allowable exceptions for releasing warrants, accompanied by agency justification and support.

Authorization for Payroll Adjustments should be Documented

State Payroll periodically adjusts employee payroll information to correct data entry errors or change employee withholding contributions, per agency request. We reviewed State Payroll's procedures for completing payroll adjustments and found five of twenty-five payroll adjustments did not include documented authorization.

EDP guidelines suggest management provide documented authorization for transactions entered in the State Payroll system to ensure proper data entry. Without documented agency authorization, State Payroll personnel may misinterpret agency requests and inappropriately adjust payroll transactions. We believe State Payroll should require documented agency authorization to ensure proper adjustment of payroll transactions.

Chapter I - Introduction

Introduction

We performed an annual electronic data processing (EDP) audit of the state's centralized data processing systems. We reviewed centralized controls over the state's mainframe computer and three computer based applications: State Payroll, Warrant Writer, and the Statewide Budgeting and Accounting System (SBAS).

During this year's audit, we performed audit work at the Department of Administration which maintains the state's mainframe, State Payroll, and SBAS. We also performed audit work at the State Auditor's Office which has primary responsibility for Warrant Writer. During our audit we gathered information, evaluated controls, and identified risks related to these systems. The controls we identified and tested are relied upon by financial-compliance, performance, and EDP audits covering fiscal year 1993-94.

Organization of Report

We organized the report into three chapters. Chapter I contains the introduction, background information, and audit objectives. Chapter II discusses our review of general controls applicable to the Department of Administration's Information Processing Facility. Chapter II also includes our application review of the department's SBAS and State Payroll mainframe computer applications. Finally, chapter III discusses our review of application controls for the Warrant Writing system, operated by the State Auditor's Office.

EDP Audit General and Application Controls

An EDP audit involves a review of management's internal controls implemented to protect assets and limit losses. In an automated environment the procedures for reviewing controls are different from those used in a manual environment. However, the objective of ensuring the reliability of controls is still the same. A general control review includes an examination of the following controls:

Organizational - apply to the structure and management of the computing and information services facility. Specific types of organization controls include segregation of duties, assignment of responsibilities, rotation of duties, and supervision.

Procedural - operating standards and procedures which ensure the reliability of computer processing results and protect against processing errors.

Hardware and Software - controls within the operating system software and hardware which monitor and report system error conditions.

System Development - oversight and supervisory controls imposed on development projects. Controls include feasibility studies, development, testing and implementation, documentation, and maintenance.

Physical Security - physical site controls including security over access to the computer facility, protection devices such as smoke alarms and sprinkler systems, and disaster prevention and recovery plans.

Electronic Access - controls which allow or disallow user access to electronically stored information such as data files and application programs.

A general control review provides information regarding the ability to control EDP applications. Application controls are specific to a given application or set of programs that accomplish a specific objective.

Application controls consist of an examination of the following controls and objectives:

Input - Ensure all data is properly coded to machine language, all entered data is approved, and all approved data is entered.

Processing - Ensure all data input is processed as intended.

Output - All processed data is reported and properly distributed to authorized individuals.

A review of the application documentation and audit trail is also performed. Applications must operate within the general control environment in order for reliance to be placed on them.

Audit Objectives

The objectives of this EDP audit were to determine the adequacy of:

1. General controls specific to the state mainframe computer.
2. Application controls over data processed by the SBAS, State Payroll, and Warrant Writer applications.

Audit Scope and Methodology

The audit was conducted in accordance with government audit standards. We compared existing general and application controls against criteria established by the American Institute of Certified Public Accountants (AICPA), General Accounting Office (GAO), and the EDP industry.

We reviewed Department of Administration's general controls related to the state mainframe environment. We interviewed department personnel to gain an understanding of the hardware and software environment at the Department of Administration. We also examined documentation to supplement and confirm information obtained through interviews.

We examined procedures within the mainframe environment which ensure computer processing activities are controlled. For example, we determined if mainframe equipment is maintained in a secured area and access is limited to authorized personnel. We also reviewed job control procedures to determine if the procedures ensure integrity of all system processing.

We conducted application reviews over State Payroll, Warrant Writer, and SBAS. We interviewed employees of the Department of Administration and the State Auditor's Office to evaluate policies and procedures. We reviewed input, processing, and output controls for these systems. We also reviewed supporting documentation to determine if controls over data are effective as well as adequate to ensure the accuracy of data during processing phases.

Controls over centralized operations are supplemented by controls established at user agencies. We did not review controls established by user agencies.

Compliance

We determined compliance with applicable state laws and rules and Montana Operations Manual policies. Except as discussed on page 13, we found the Department of Administration and the State Auditor's Office to be in compliance with applicable laws and state policy.

Prior Audit Recommendations

Our prior audit report for fiscal year 1992-93 included two recommendations still applicable to the Department of Administration's State Payroll application. We reviewed the status of these recommendations during our audit and determined the department concurred with and implemented each recommendation.

Our prior audit report also included five recommendations applicable to the Warrant Writer application operated by the State Auditor's Office. The office concurred with our recommendations. During our audit, we determined the office implemented four recommendations and partially implemented one. The partially implemented recommendation concerns Warrant Writer disaster recovery procedures.

Although the State Auditor's Office has partially completed Warrant Writer disaster recovery procedures, the office should consider establishing recovery procedures at the hotsite location, as discussed on page 6.

Chapter II - Department of Administration

Introduction

The Department of Administration operates the Information Processing Facility, the Statewide Budgeting & Accounting System (SBAS) application, and the State Payroll application. This chapter summarizes our review of general controls over the Information Processing Facility and application controls over SBAS and State Payroll.

Information Processing Facility

The Department of Administration's Information Services Division (ISD), provides data processing services for use by state agencies. Central data processing services include: central mainframe computer processing; design, development, and maintenance support of data processing applications; and disaster recovery facilities for critical data processing applications. Processing is performed on an IBM 3090 computer operating 24 hours a day except during scheduled system maintenance.

General controls are developed by management to ensure computer operations function as intended. In our review of ISD's general control environment, we found the general controls provide for controlled application processing on the mainframe computer system. However, as discussed in the following sections, we identified physical security and electronic access control issues which could compromise the department's ability to provide continuous processing services. We also noted weaknesses which could reduce the effectiveness of ISD services provided to computer users.

Physical Security

Physical security controls provide security against accidental loss or destruction of data and program files or equipment and ensure continuous operation of EDP functions. Physical security controls include: safeguard of files, programs and documentation; physical access over the computer facility; and a plan or method to ensure continuity of operations following major destruction of files or hardware breakdown.

We reviewed existing physical controls in place at the Information Processing Facility. The department has installed computer

hardware on a raised floor, smoke alarms function properly, air conditioning maintains controlled computer room temperature, and the power supply meets computing equipment needs. However, the following sections discuss areas where the department could improve physical security controls.

ISD Should Complete a Disaster Recovery Plan

The Department of Administration received funding from the 1991 Legislature to adequately design and implement a contingency plan, which included a "hotsite" and the appropriate backup equipment. In February 1992, ISD established a five year contract for a backup hotsite with Weyerhaeuser Information Systems in Seattle, Washington. With an annual subscription cost of $28,435, the hotsite agreement provides ISD an alternative location and equipment necessary to recover mainframe computer operations. The contract also provides the ability to recover agency-owned applications such as the Payroll/Personnel/Position Control (PPP) system and the Statewide Budget Accounting System (SBAS).

Each year we review the status of ISD's disaster recovery plan. We determined ISD has not completed a recovery plan or included agency applications in its recovery procedures. Although ISD has not completed a disaster recovery plan, it continues to improve its ability to recover mainframe computing operations. In September 1993, ISD performed testing at the hotsite for recovery of mainframe operating system hardware and software. In November 1994, ISD will test its telecommunications network, which agencies use to connect to the mainframe from remote locations. Operating system hardware, software, and telecommunications represent the basis for the mainframe computing services ISD provides to state agencies. However, these services could not be utilized following a disaster unless state agencies establish hotsite recovery procedures for their mainframe application programs and data.

A disaster, when associated with a computer center, relates primarily to the disruption or destruction of computer resources. Disasters to a computer facility take many forms. Minor operational errors, temporary loss of power, and total destruction of the computer center may each constitute a disaster. The key to recovery from the many different levels of disruption is a

documented recovery plan. Necessary disaster recovery procedures depend on management's "risk assessment" of how long the organization can operate without processing, management's backup procedures, and cost.

ISD's disaster recovery plan should, at a minimum, include:

-- An inventory of current mainframe applications, operating system programs, telecommunications programs, networks, and hardware.

-- An analysis to determine application criticality and the impact of loss of the application.

-- An analysis to determine application recovery priority.

-- Identification, involvement, and commitment of employees responsible for recovering mainframe operating system hardware and software, and agency applications.

-- Definition of application requirements including personnel, hardware, system support programs, communications, data, special forms, negotiable instruments, etc.

We believe ISD should complete its disaster recovery plan by including agency applications and documenting recovery procedures. ISD, as the major "supplier" of data processing services in the state, should assume the responsibility of assisting agencies in the development of recovery plans. This close assistance would ensure recovery procedures meet agency needs and contain necessary information for ISD and agencies to process critical applications at an off-site facility.

Since contracting with Weyerhaeuser, ISD's Computing Operations bureau has placed priority on recovering mainframe hardware, operating system software, and telecommunications. As a result, ISD has not established application recovery priorities or coordinated efforts with state agencies for application recovery. However, ISD employees indicated the department has established procedures to complete a recovery plan by June 1995. The director of the Department of Administration, with assistance from the Information Technology Advisory Council, should identify and establish priorities for

applications which must be recovered to continue state government operations following a disaster.

Recommendation #1

We recommend the department:

A. Complete and document a formal disaster recovery plan.

B. Request agency participation and provide assistance to state agencies for development of application recovery procedures.

Restricted Access to the Information Processing Facility should be Improved

During fiscal year 1993-94, Information Services Division used an electronic password system to restrict access to the Information Processing Facility. To access the facility individuals entered a password through a keypad at the processing facility entrance. In July 1994, ISD installed a replacement access control system to provide additional security and record individual access to the facility. We evaluated ISD's physical access controls in place during fiscal year 1993-94, and identified the following concerns.

ISD has not established procedures to remove employee access as soon as no longer required. We interviewed ISD employees and reviewed position descriptions to evaluate the need for employee access to the processing facility. We found one of ten employees no longer required the access, because the employees' job duties had changed. In addition, as discussed below, we also determined unauthorized individuals could bypass the electronic access system to enter the facility.

We determined individuals, who do not work for ISD, could bypass the electronic access system by using a key at the facility entrance. The Department of Administration's General Services Division, which oversees capital complex maintenance and security, issues grandmaster keys to its employees and

contractors. The grandmaster key provides access to several buildings within the capital complex. As a result, the grandmaster key provides unauthorized individuals direct access to the computer facility. For example, elevator service contractors and grounds-maintenance personnel can bypass ISD's electronic access system to enter the computer facility.

Industry standards suggest management restrict computer facility access to individuals who require access while performing their job duties. Unauthorized individuals could accidentally or intentionally destroy operating system hardware and disrupt computing operations.

We believe ISD should establish procedures to remove employee access as soon as no longer required. An ISD employee indicated the division evaluated employee access privileges when installing the new access control system. The employee also noted the division has changed the locks to the processing facility to restrict unauthorized access with the grandmaster key.

Recommendation #2

We recommend the department establish procedures to limit physical access to the Information Processing Facility to individuals who require the access.

Physical Access to Operating System Documentation

Operating system documentation includes installation guidelines and procedures, system configurations, user-written modifications, software installation programs, etc. ISD's Operating System Support programmers refer to system documentation daily and during periodic modifications or installations of operating system software. For example, when performing software installations, operating system programmers document installation procedures and system specifications.

During our audit, ISD remodeled office space to more efficiently use existing work areas. We determined ISD's operating system

documentation is no longer restricted from unauthorized access. Prior to remodeling, ISD's Operating System Support programmers stored system documentation within their work area and access to the office, during non-working hours, was restricted. However, since removing a wall to enlarge the work area, additional employees have unrestricted access to operating system documentation.

EDP guidelines suggest management restrict access to operating system documentation to individuals who require access to perform job duties. Unrestricted access could allow unauthorized individuals to change operating system specifications or destroy installation documentation. We believe ISD should consider an alternative storage area or secure operating system documentation in locked storage cabinets.

Recommendation #3

We recommend the department restrict access to operating system documentation to employees who require access to perform job duties.

Physical Inventory of Tapes at Storage Facility

We reviewed ISD's procedures which ensure software and data are backed up regularly and stored at a secure off-site location. Twice each week, ISD employees back-up all mainframe operating system software, application programs, and data to cartridges, which they store at an off-site facility. ISD stores both mainframe and agency-owned programs and data at the off-site location.

We determined ISD has not completed an inventory of back-up data stored at the off-site facility in over three years. EDP guidelines suggest management perform an annual physical inventory to verify assets and ensure accuracy of inventory records. A complete physical inventory provides management the ability to verify backup data location and existence. Without a complete inventory, ISD may be unable to locate critical data

following a disaster. ISD personnel indicated they disposed of prior inventory records while reorganizing offices.

During our audit ISD purchased an electronic tape management system which employees use to identify and document back-up tape location. ISD employees noted they are now using the tape management system and completed an inventory at the off-site facility following our review. We believe the electronic system should enable ISD employees to efficiently complete an annual physical inventory of backup data stored at the offsite facility.

Recommendation #4

We recommend the department complete and document a formal annual inventory of back-up data stored at the off-site storage facility.

Electronic Access Controls over Operating System Software

The Department of Administration's Information Services Division uses ACF2 (Access Control Facility) software to control computer user access to mainframe application programs and data.

We reviewed electronic access controls over mainframe operating system software. The following section identifies an area where the department could improve electronic access security over the mainframe operating system files and programs.

Database Programmer Access to Operating System

ISD's Systems Support Bureau employs database application programmers who perform application modification duties on the mainframe computer. The database applications programming personnel periodically modify or install database software which communicates with mainframe operating system files. We determined three database application programmers have unnecessary write access to the mainframe operating system programs.

Database application programmers should not have write access to mainframe operating system software. Industry standards suggest only personnel responsible for maintaining operating system software have access to operating system files. ISD's Operating System Support division employs systems programmers who code installation-defined system modules and maintain the operating system. Because the database application programmers do not perform maintenance duties there is no need to grant access to the operating system libraries and program modules.

Although database programmer activity within the operating system library is recorded and monitored, systems programmers may not detect unauthorized operating system changes. The write access allows database programmers to accidentally or purposefully manipulate operating system parameters which could cause breach of security, remove audit trails, and corrupt applications. The systems programmers could perform necessary changes for the database programmers, thereby eliminating the risk of unauthorized operating system changes.

Recommendation #5

We recommend the department remove database application programmer access to the operating system library.

Organizational Controls

Organizational controls provide for effective operation, structuring, and management of computer center operations and services. Computing Operations Bureau's primary function is to provide mainframe computing service to state government agencies. We found ISD's operations provide effective and reliable mainframe processing service to computer users. However, we noted an area where Computing Operations Bureau could improve controls to ensure mainframe services continue to meet user needs.

Employee Performance Evaluations

We determined Computing Operations Bureau employees have not received performance evaluations in accordance with state policy. We reviewed personnel files for eleven bureau employees, including computer operations specialists and operating system specialists. As of June 1994, seven of the eleven employee evaluations were overdue between two to nine months.

State policy, section 2.21.6411, Administrative Rules of Montana, requires management evaluate and document employee work performance at least once per year. Annual performance evaluations provide the employee an opportunity to assess progress and improve performance. Evaluations also allow management to monitor employee performance, make suggestions for improvement, and support decisions regarding advancement, demotion, or termination.

Management noted they recognize the importance of annual employee evaluations but sited employee retirements and changes in employee responsibilities as reason for overdue performance appraisals. The Computing Operations Bureau indicated ISD has issued a directive to complete performance appraisals for all employees by September 1994.

Recommendation #6

We recommend the department complete performance appraisals in accordance with state policy.

Statewide Budgeting and Accounting System

The Department of Administration, Accounting Bureau, operates the Statewide Budgeting and Accounting System (SBAS). SBAS is an accounting system which provides financial information used to review and control agency financial transactions. The system also provides agency management budgetary control data used for decision making. SBAS provides uniform accounting and reporting for all state agencies by showing receipt, use, and

disposition of all public money and property in accordance with generally accepted accounting principles (GAAP).

We performed an application review of SBAS. We reviewed input, processing, and output controls over SBAS. Overall, we determined controls over SBAS were effective, as well as adequate, to ensure data integrity during processing phases for fiscal year 1993-94. However, as noted below, we determined the Accounting Bureau should establish internal policies to ensure continued application of SBAS processing controls.

The Accounting Bureau should Establish Formal Procedures

The SBAS application produces a daily report of accounting transactions which cause an accounting entity cash balance to become negative. We reviewed SBAS processing controls which ensure warrants are not issued unless the accounting entity cash balance is positive. We determined Accounting Bureau personnel can override the application controls to allow warrant processing in special circumstances. However, the Accounting Bureau has not established formal procedures for releasing warrants when cash is negative.

During fiscal year 1993-94, the Accounting Bureau periodically released warrants for Department of Commerce and the State Compensation Mutual Insurance Fund when the accounting entity cash balance was negative. Accounting Bureau personnel indicated they released warrants upon verbal agency request contingent upon subsequent cash receipt.

Section 17-2-107, MCA, requires the Department of Administration to adopt procedures to insure proper accounting of state treasury funds. If an expenditure is necessary but the cash balance is insufficient, the department may authorize a temporary loan, provided there is reasonable evidence the agency can repay the loan within one year. However, the Accounting Bureau does not follow this process when releasing warrants per agency request.

Controls established within SBAS are intended to protect the state treasury and prevent overexpended cash balances. The Accounting Bureau's current procedure may allow inappropriate

fiscal activity by state agencies. For example, the State Compensation Mutual Insurance Fund could issue monthly workers' compensation benefit payments and neglect to transfer funds necessary to cover the warrants. We believe the Accounting Bureau should document allowable exceptions for releasing warrants, accompanied by agency justification and support.

Recommendation #7

We recommend the department document formal procedures for releasing warrants when an accounting entity cash balance is negative.

State Payroll System

The State Payroll System, operated by Department of Administration, processes payroll for state agencies and the University System. The State Payroll System is also referred to as the Payroll/Personnel/Position Control system (P/P/P). The payroll component issues and tracks state of Montana employees' wage and benefit payments. The payroll component also calculates payroll deductions, leave and service adjustments, automatic salary increases, and direct bank deposits upon request. The personnel component records detailed information about each state employee such as birth, sex, disability, and emergency notification for each employee. The personnel database also includes information to verify compliance with state and federal labor laws. The position control component provides management with information necessary for budgeting purposes and includes information on employee position number, grade, classification code, date of hire, and longevity.

Our EDP audit was limited to application controls applicable to payroll transactions processed through the State Payroll System. We determined input, processing, and output controls over the State Payroll System were effective for fiscal year 1993-94. However, we found an area where State Payroll could enhance

controls to further ensure data security and integrity. The following section summarizes our finding.

Authorization for Payroll Adjustments should be Documented

State Payroll periodically adjusts employee payroll information to correct data entry errors or change employee withholding contributions. For example, agencies may request an employee payroll adjustment to increase tax withholding or decrease contributions to flexible spending accounts. If the request applies to a previously processed pay period, or requires correction immediately preceding payroll processing, State Payroll personnel complete the adjustment for the agency.

Generally, State Payroll requires agencies to follow up verbal adjustment requests with documented authorization. Documented authorization may include a note authorized by agency personnel. In some cases, the employee may initiate the request by reimbursing State Payroll for wages which should have been deducted. In this case, documented authorization may be limited to the employee's personal check or the employee may return the payroll warrant. We reviewed State Payroll's procedures for completing payroll adjustments and identified instances where State Payroll did not have documented authorization for payroll adjustments.

Five of twenty-five payroll adjustments we reviewed did not include documented authorization. Two adjustments involved reimbursing employees for deductions made to the employees flexible spending accounts. Another adjustment required correcting an employees' contribution to a retirement fund. For the remaining two adjustments, State Payroll personnel corrected agency calculations of employee withholding for employees retiring in December 1993.

EDP guidelines suggest management provide documented authorization for transactions entered in the State Payroll system to ensure proper data entry. Without documented authorization, State Payroll personnel may misinterpret agency requests and inappropriately adjust payroll transactions. State Payroll personnel indicated they do not consider documented agency authorization necessary for all adjustments. We believe State

Payroll should require documented agency authorization, in acceptable form, to ensure proper adjustment of payroll transactions.

Recommendation #8

We recommend the department obtain documented agency authorization for payroll adjustments.

Chapter III - State Auditor's Office

Introduction

The State Auditor's Office operates the Warrant Writer System which processes warrants for state government. This chapter summarizes our audit of application controls over the Warrant Writer System.

Warrant Writer System

The Warrant Writer system controls creation and distribution of most state warrants and the redemption of all state warrants. The system accounts for state warrants issued, outstanding, and redeemed.

The State Auditor's Office and the Department of Administration jointly operate and maintain Warrant Writer. However, the State Auditor's Office is primarily responsible for the system. Department of Administration initiates warrant writing and reconciles issued warrants to SBAS. The State Auditor's Office prepares warrants, distributes warrants, and reconciles warrants outstanding to SBAS. Both agencies jointly control warrant redemption.

We performed an application review of the Warrant Writer system. We reviewed input, processing, and output controls over Warrant Writer. Overall, we determined controls over Warrant Writer are effective, as well as adequate, to ensure accuracy of data during processing phases.

Prior Audit Status

During our prior audit, we issued five recommendations to the State Auditor's Office. Our recommendations concerned electronic access controls, warrant distribution procedures, physical security over warrants, and disaster recovery procedures. We determined the office completely implemented four recommendations and partially implemented one. The partially implemented recommendation concerns establishing disaster recovery procedures for the Warrant Writer system in accordance with state policy. Although the State Auditor's Office has not completed a recovery plan, the office has evaluated Warrant Writer system requirements and defined personnel responsibilities. We believe the State Auditor's Office

is prepared to work with the Department of Administration to complete its disaster recovery plan. Therefore, we make no recommendation at this time.

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

MARC RACICOT, GOVERNOR

STATE OF MONTANA

(406) 444-2032
FAX: 444-2812

MITCHELL BUILDING
PO BOX 200101
HELENA, MONTANA 59620-0101

October 31, 1994

Scott A. Seacat
Office of the Legislative Auditor
Room 135, State Capitol
P. O. Box 201705
Helena, MT 59620-1705

Dear Mr. Seacat:

We have reviewed the recommendations pertaining to the EDP Audit of the Information Processing Facility and Central Applications dated November 1994. Our responses follow:

RECOMMENDATION #1

WE RECOMMEND THE DEPARTMENT:

A. COMPLETE AND DOCUMENT A FORMAL DISASTER RECOVERY PLAN.

RESPONSE

We concur. ISD continues to address disaster recovery as an integral part of managing the data center. The disaster recovery plan is undergoing its third major revision and is scheduled for completion by June, 1995, with a draft version scheduled to be available by December 30, 1994. Currently ISD is collecting data on computer/mainframe operations, cabling configurations, hardware/software inventories, database application documentation, policies and procedures, staffing configurations, salvage team vendors, etc. Components of the comprehensive disaster recovery plan will include:

Disaster Recovery Teams
Disaster Recovery Plans
Coordinator/Manager's Plan
Business Continuation Plan

Salvage Team Plan
Hot Site Plan
Relocation Plan
Transition Plan
Testing and Updating the Plan

All of the disaster plan components listed in the recommendation will be included in the revised plan.

B. REQUEST AGENCY PARTICIPATION AND PROVIDE ASSISTANCE TO STATE AGENCIES FOR DEVELOPMENT OF APPLICATION RECOVERY PROCEDURES.

RESPONSE

We concur. ISD will work with agencies through ITAC in developing the revised disaster recovery plan. ISD will then provide assistance to agencies in developing their application recovery plans. This is scheduled to be completed by June 30, 1995.

RECOMMENDATION #2

WE RECOMMEND THE DEPARTMENT ESTABLISH PROCEDURES TO LIMIT PHYSICAL ACCESS TO THE INFORMATION PROCESSING FACILITY TO INDIVIDUALS WHO REQUIRE THE ACCESS.

RESPONSE

We concur. We will establish procedures and implement a system that assures timely review of all ISD personnel who are allowed physical access by the respective employee's bureau chief. This system will also assure timely review of non-ISD personnel access by ISD's Central Security Officer. This system is scheduled to be in place by January 1, 1995.

RECOMMENDATION #3

WE RECOMMEND THE DEPARTMENT RESTRICT ACCESS TO OPERATING SYSTEM DOCUMENTATION TO EMPLOYEES WHO REQUIRE ACCESS TO PERFORM JOB DUTIES.

RESPONSE

We concur. ISD management will identify those system documentation materials that represent an exposure to systems integrity through unauthorized personnel access. These materials will be kept locked, with access limited to bureau personnel requiring them to perform their job duties. This security procedure will be in place by January 1, 1995.

RECOMMENDATION #4

WE RECOMMEND THE DEPARTMENT COMPLETE AND DOCUMENT A FORMAL ANNUAL INVENTORY OF BACK-UP DATA STORED AT THE OFF-SITE STORAGE FACILITY.

RESPONSE

We concur. We agree that a complete physical inventory of all volumes of magnetic tape should be completed annually. This inventory should include the magnetic tapes housed within the data center tape storage area as well as the off-site storage facility. We will implement a formal annual inventory process, the first of which is scheduled to be completed by February 1, 1995.

RECOMMENDATION #5

WE RECOMMEND THE DEPARTMENT REMOVE DATABASE APPLICATION PROGRAMMER ACCESS TO THE OPERATING SYSTEM LIBRARY.

RESPONSE

We concur. Access authority for operating system libraries has been removed for database support personnel.

RECOMMENDATION #6

WE RECOMMEND THE DEPARTMENT COMPLETE PERFORMANCE APPRAISALS IN ACCORDANCE WITH STATE POLICY.

RESPONSE

We concur. An effort is currently underway to provide all ISD employees with a performance appraisal for the appraisal year ending 09/30/94 and with new performance standards for the appraisal year beginning 10/01/94.

RECOMMENDATION #7

WE RECOMMEND THE DEPARTMENT DOCUMENT FORMAL PROCEDURES FOR RELEASING WARRANTS WHEN AN ACCOUNTING ENTITY CASH BALANCE IS NEGATIVE.

RESPONSE

We concur. We are in the process of writing formal procedures and will have them in place by December 1, 1994.

RECOMMENDATION #8

WE RECOMMEND THE DEPARTMENT OBTAIN DOCUMENTED AGENCY AUTHORIZATION FOR PAYROLL ADJUSTMENTS.

We concur. Effective with the October 25, 1994 payday, we have changed our procedures to ensure that we have documentation from agencies for payroll adjustments.

We appreciate the opportunity to interact with your staff on these issues.

Sincerely,

Lois Menzies

Lois Menzies
Director

STATE AUDITOR
STATE OF MONTANA

Mark O'Keefe
STATE AUDITOR

COMMISSIONER OF INSURANCE
COMMISSIONER OF SECURITIES

October 14, 1994

Mr. Rich McRae, EDP Audit Senior
Office of the Legislative Auditor
PO Box 201705
Helena, MT 59620-1705

Dear Mr. McRae:

I have reviewed your draft copy of the EDP audit on the State Auditor's Warrant Writer System. I concur with your suggestion that we continue to work with the Department of Administration on a disaster recovery plan for the Warrant Writer Application. My staff is currently working with ISD and other state agencies to develop a plan for recovery of our process.

I would like to thank you and your staff for your effort to help us improve our data processing procedures. Your staff showed excellent knowledge of our application and offered constructive suggestions on numerous occasions. We appreciate the professional manner used by your staff in completing this important audit.

Sincerely;

Thomas L. Crosser, Deputy
Fiscal Control and Management

Mitchell Building/PO Box 4009/Helena, Montana 59604-4009/(406) 444-2040/1-800-332-6148/FAX: (406) 444-3497